HUMAN ERROR ANALYSIS FOR HUMAN-RATED SPACE SYSTEMS

Alan Hobbs [1], John O'Hara[2], Cynthia Null [3], Charles Dischinger [4]

[1]*SJSU Research Foundation, NASA Ames Research Center, Moffett Field, CA, 94039, USA. alan.hobbs@nasa.gov*
[2] *Brookhaven National Laboratory, Upton, NY 11973, USA. ohara@bnl.gov*
[3] *National Aeronautics and Space Administration, Langley Research Center, Hampton, VA 23666, USA cynthia.h.null@nasa.gov*
[4] *National Aeronautics and Space Administration, Marshall Space Flight Center, Huntsville, AL 35808, USA. charles.dischinger@nasa.gov*

ABSTRACT

Humans bring unique capabilities to space systems and contribute to mission success in a manner that cannot be matched by machines. Nevertheless, from time to time, human error can present a threat to system performance, and system designers must anticipate and manage this risk. NASA's Human-Rating Requirements for Space Systems call for program managers to conduct a human error analysis (HEA) during system development but does not specify how to do this. In 2018, NASA's Engineering and Safety Center asked the authors to develop a guidance document on HEA. The resulting position paper outlines a suggested method for HEA and makes it clear that error analysis is about identifying and mitigating problems at a system level, and not about finding fault with individuals. Error management strategies must be directed at error-producing conditions, thereby reducing the likelihood of human error, while retaining the positive contribution that humans make to system operations.

1. INTRODUCTION

Operational personnel make a vital contribution to system safety, especially in novel situations where human intelligence and adaptability can help manage and mitigate unforeseen circumstances. However, despite the positive human contribution to system operations and maintenance, human errors sometimes occur. When they do, they can pose a threat to system safety and performance.

In 2014, a commercial re-usable suborbital rocket broke up during a test flight when a crewmember prematurely unlocked a feather system designed to increase drag during re-entry. As a result of aerodynamic forces, the unlocked feather system deployed during ascent, and the spacecraft broke-up in-flight. One member of the two-person crew was fatally injured, while the other survived with serious injuries. The spacecraft was being operated under an experimental permit issued by the Federal Aviation Administration (FAA) Office of Commercial Space Transportation. One of the regulatory requirements was that the permit holder must identify and describe hazards resulting from human error. However, the FAA issued a waiver from this requirement, and the operator apparently assumed that crewmembers would perform the feather unlocking task correctly every time. An investigation by the National Transportation Safety Board (NTSB) concluded that the probable cause of this accident was the operator's "failure to consider and protect against the possibility that a single human error could result in a catastrophic hazard …" The NTSB noted that there was a lack of guidance for commercial space operators on how to consider human error as part of a hazard analysis [1].

The United States National Aeronautics and Space Administration (NASA) recognizes that if not managed appropriately, human error can present significant threats to space transport systems. Consequently, NASA's Human-Rating Requirements for Space Systems [2] requires Program Managers to conduct a human error analysis (HEA) for all mission phases including flight operations, ground processing, and launch preparation. This analysis is described as a *qualitative* analysis, in that it is directed at identifying potential errors and their effects, rather than placing probabilities on errors. HEA augments and interacts with other human-rating activities such as hazard analysis, workload assessment, task analysis, and the application of human factors design standards.

In 2018, NASA's Engineering and Safety Center recognized the need for guidance on the conduct of a HEA and tasked the authors with developing such a document. This paper summarizes the position paper that resulted from that work [3].

2. CONDUCTING A HUMAN ERROR ANALYSIS

The purpose of a human error analysis is to seek out vulnerabilities where human performance could pose a threat to the mission and mitigate problems at an integrated system level, including hardware, software, personnel, facilities, processes, and procedures. Although the term "human error" sometimes carries connotations of judgment or blame, HEA is not about finding fault with individuals.

We propose that the HEA process can consist of seven steps, each of which is described in the following subsections. Note that the process as described in this paper represents one possible way to approach a qualitative HEA and is certainly not the only feasible approach.

2.1 The HEA team

The HEA should be conducted by a team comprising personnel with diverse, multidisciplinary expertise, experience, and perspectives. In addition to the human factors specialist, the team should include Subject Matter Experts (SMEs) from the system's user community who will be familiar with the systems and tasks. For example, if the HEA is considering a ground processing task, the HEA team may include experienced ground processing personnel in addition to a human factors specialist and design engineers. Even when the tasks are new and associated with new system designs, personnel who have performed similar tasks with predecessor systems are likely to provide valuable insights. The HEA team should also have access to members of the design team in order to understand the design as it progresses and resolve questions.

The HEA team should maintain close bi-directional communication with the design team throughout the design process and should be ready to provide assistance when needed to identify and address potential human errors. However, because it can be difficult for designers to recognize problems in their own designs, the HEA team also provides an assessment of the system independent of the design team. The HEA team therefore needs access to design documentation as well as evaluations and analyses that can help identify functions that rely on human performance and tasks during which human errors could occur.

2.2 Identify functions and tasks, and screen for importance

The purpose of this step is to (a) identify critical functions that, if lost, could lead to catastrophic events, and (b) identify the high-level tasks that must be performed to accomplish the critical functions.

Systems accomplish their missions through a set of functions. Functions are described in terms of high-level goals, without reference to how they are accomplished. For example, one crewed-spacecraft function is "maintain cabin habitability." As the design develops, functions are further decomposed into the systems and actions needed to accomplish the function.

Functions may be accomplished by machine actions (e.g., automatic systems), human actions (e.g., tasks performed by personnel), or through a combination of human and machine actions.

The HEA team may obtain information on system functions and tasks from a variety of sources, including system operations documentation, input from subject matter experts, including operations and maintenance personnel, and analyses conducted as part of other systems engineering activities.

In the early stages of concept development, it may be appropriate to perform the HEA at a broad level of granularity at the level of functions. Such an analysis may describe errors in broad terms. Examples are: "Function not performed" or "Function performed incorrectly." Tab. 1 provides a hypothetical example of an early-stage HEA that occurs at a broad level.

Table 1. Hypothetical example of an early-stage HEA

> Prior to the Preliminary Design Review, a general list of functions that may require human input during flight is obtained by the HEA team. A detailed list of crew tasks is not yet available, but the HEA team identifies that crew members will be involved in certain critical functions during the initial ascent, which will require them to interact with screen displays.
>
> The HEA team identifies that vibration during ascent stage could lead to crew errors when reading text on screen displays as conceived in the initial concept. The HEA team reviews existing research on the topic and recommends the adoption of a larger font size.

Early HEAs are critically important, as they have the potential to identify problems that can be addressed at a time when design changes are least disruptive. As the design process proceeds, human actions will become progressively more defined and more fine-grained HEA will be possible.

The number of tasks associated with a system's construction, operation, and maintenance can be immense. NASA requires the HEA to consider errors that could result in a catastrophic outcome, defined as an event that could result in the death or permanent disability of an occupant of a crewed space system. Therefore, a screening process must be applied to identify critical functions and tasks where incorrect performance could lead to a catastrophic outcome.

One approach to understanding complex systems is STPA (System-Theoretic Process Analysis). The STPA approach reveals system processes by modelling control structures, including those that involve humans. The approach can help to identify areas of system operation where human actions are critical [4].

Functions and associated tasks not determined to be critical can generally be screened out and not considered further. For critical functions, the analyst should determine which of the identified high-level tasks are necessary for function accomplishment. Those that are necessary are screened in for further analysis. Those that are not necessary are screened out from further analysis.

Each HEA team must develop its own internal guidelines to determine which tasks should be screened in for analysis, although the team should retain the flexibility to examine additional tasks if judged necessary. For example, the team may decide to screen in situations where a catastrophic outcome could result from a single inadvertent operator action, including responses to system failures or emergency conditions.

Identifying potential errors in ground processing and assembly operations can be particularly challenging. Incorrectly performed tasks may be difficult to identify and may lie dormant for many years, as in the following case.

In 2004 maintenance personnel found that gears in the rudder/speed brake of the space shuttle Discovery had been installed in reverse during initial assembly in the late 1970s or 80s. The shuttle had flown 28 missions during which the flawed assembly continued to perform its function. A failure of the rudder/speed brake could have resulted in loss of the shuttle and its crew [5].

The large number of ground processing and assembly operations means that every interaction by ground personnel with flight hardware cannot possibly be subject to a thorough HEA. The HEA team may choose to use screening guidelines as shown in the following examples:

- Screen in assembly, test, and integration tasks that occur at the launch facility.
- Screen in tasks at the level of interactions with line replaceable units (LRUs).
- Screen out most interactions with components or parts below the level of LRUs.
- Screen out ground processing actions that are followed by a full functional test prior to launch.
- Screen out ground processing actions if failure to perform correctly would be obvious and correctable prior to launch.

2.3 Detailed task analysis

Task analysis refers to a broad family of techniques used to characterize and understand human interactions with systems and the detailed requirements needed to accomplish desired goals. The methods can range from formal analysis methods, such as hierarchical task analysis, to less formal methods such as task observations, and walk-throughs of tasks by operations personnel. Task analysis provides a robust context to understand how critical human tasks are performed and, potentially, what conditions may lead to human errors.

The analyst may not have to conduct the task analysis as part of the HEA if task analyses have been performed as part of other Human System Integration (HSI) activities, such as the Master Task List for in-flight activities, or a task analysis created for a human reliability analysis (HRA). The initial steps of HRA are similar to the steps required for HEA. In each case, the tasks assigned to humans are defined, and then potential errors are identified. However, while HRA moves on to assign probabilities to errors, HEA remains a qualitative analysis focused on identifying and responding to the threat posed by specific errors.

Augmenting the task descriptions will require the involvement of SMEs. At a minimum, personnel who are expected to perform the tasks should be consulted. If detailed task analyses are not available, they should be conducted to support the HEA. This may particularly apply to ground operations.

The task analyst must consider not only the ways tasks should be performed, but also how work might actually be performed under the demands of the work environment. At times, operational personnel will interact with systems in ways that were not intended or foreseen by system designers, procedure developers, and trainers. For this reason, HEA must also consider some human actions that are not linked to specific tasks, including undesired human interactions with an item of equipment that could have been reasonably predicted by the designers. (e.g., using a non-weight bearing structure as a foothold).

For example, a U shaped flexhose near a window of the International Space Station was used as a handhold. Damage to the flexhose caused a slow air leak. The leak posed no immediate danger, but it took astronauts two weeks to locate its source [6].

Many traditional task analysis methods focus on outward behaviors (i.e., physically observable actions) [7]. However, all tasks involve cognitive activities to some extent, and some (such as fault diagnosis) are almost entirely cognitive. As operations become more automated, the role of personnel is becoming less activity-oriented and more reliant on cognitive activities that must be inferred rather than observed directly.

If the task is determined to be critical (i.e., if an error during the task could result in a catastrophic event), it may be necessary to analyze the task further using cognitive task analysis techniques. Cognitive tasks analysis methods are directed at identifying the unobservable, but crucial, mental processes involved in task performance. This need not be overly complicated and may involve identifying (1) the sources of information relied on by the task performer, (2) the mental processes, memory demands, and decisions made during task performance, and (3) the actions required to accomplish goals [8].

2.4 Describe the task context

Once detailed descriptions are available for each critical task, the HEA analyst should consider aspects of the task context that could increase the likelihood of error.

We refer to these contextual factors as error-producing conditions (EPCs). Some of these conditions are internal to the person at the time (e.g., fatigue, skill level, or stress). Others exist external to the person (e.g., environment, task, equipment). Over a century of human factors research has contributed to a vast literature on these conditions, and human factors specialists will be familiar with the state of knowledge in this field.

It is helpful to distinguish between EPCs and error traps. Most EPCs are general conditions that can increase the likelihood of error across a range of tasks. Error traps are EPCs, either alone or in-combination, that can provoke a specific error on a specific task [9]. Error traps can take the form of hardware, software, procedures, training, or other aspects of system design and operation. Examples are plugs that can be mated to the wrong connections, and procedures that require a level of precision or strength that cannot be reliably delivered under the work conditions.

Many EPCs, such as human fatigue, can never be eliminated entirely. However, in most cases, error traps can be eliminated with appropriate design.

The presence of significant EPCs can be a sign to the HEA team that the task requires close examination for potential errors. For example, recovery tasks that could be performed at sea in challenging sea states may have a heightened overall chance of error, and may therefore require more analysis than tasks performed in more forgiving conditions.

The human factors literature contains numerous lists and taxonomies of EPCs, and the intent is not to provide detailed information in this document. Tab. 2 contains sample questions concerning error-producing conditions that can be asked of personnel while reviewing or talking through the specific task to be analyzed.

Table 2. Sample questions to identify EPCs

- Is there anything about the human-system interface or equipment that could increase the likelihood of error on this task? If so, describe.
- Are there task demands, either physical or cognitive, that could increase the likelihood of error (e.g., required physical strength or reach, or cognitive demands such as reliance on memory or attention)? If so, describe.
- Could any of the procedures for this task potentially confuse the operator or otherwise lead to an error? If so, describe.
- Could the environment in which the task is performed increase the likelihood of error? If so, describe.
- Are there coordination, teamwork, or communication issues that could increase the likelihood of error on this task? If so, describe.

2.5 Identify potential catastrophic errors

Now that the task and its context has been considered, the HEA can move on to identify errors that have the potential to lead to a catastrophic event.

Guide words can help ensure that the full range of potential errors has been captured. Tab. 3 contains a generic list of errors expressed as outward behaviors, adapted from Hollnagel's Cognitive Reliability and Error Analysis Method (CREAM) [10]. Note that an error analysis at the level of outward behavior is concerned with what might happen, not with why a person might act in this way.

Table 3. Guide words to assist in identifying potential errors in terms of outward behavior

General effect	Specific effect	Explanation
Action at wrong time	Too early	An action started too early, before a signal was given or the required conditions had been established
	Too late	An action started too late
	Omission	An action was not done at all
	Too long	An action continued beyond the point where it should have been stopped
	Too short	An action was stopped prematurely
	Repeated	An action was repeated
	Reversal	The order of two neighboring actions

		was reversed
Action of wrong type	Too little force	Insufficient force
	Too much force	Excessive force
	Too much distance/magnitude	Movement taken too far
	Too short distance/magnitude	Movement not taken far enough
	Too fast	Action performed too rapidly
	Too slow	Action performed more slowly than required
	Wrong direction	Movement in wrong direction (e.g., left instead of right)
	Wrong type of movement	e.g. pulling a knob instead of turning it
Action involves wrong object	Neighbor	The object acted upon is near the object that should have been acted upon
	Similar object	The object acted upon is similar in appearance to the object that should have been acted upon
	Unrelated object	Object was used in error, even though it has no obvious relation to the object that should have been used

Adapted from Hollnagel, 1998

In certain cases, it may be helpful to augment the outward description of the error using a cognitive model of error. Cognitive models categorize errors on the basis of their presumed cognitive origins (e.g., by describing an error as a memory lapse or a failure of problem-solving) [11,12].

Compared to outward descriptions, cognitive models can provide insight into error causation and therefore may be more helpful in identifying strategies to manage error. Errors that involve the same outward observable behavior may have markedly different cognitive origins. For example, an incorrect keyboard entry may require a different design response depending on whether the action is the result of a skill-based slip or results from a knowledge-based mistake.

Even if insufficient information is available to completely categorize the error with a cognitive model, a partial conclusion, such as determining whether the task would involve automatic or controlled processing, can be useful [13].

2.6 Identify error traps

After potential errors and their contexts have been described for each task, task-specific error traps may become evident. In some cases, a single EPC can be considered to be an error trap—e.g., adjacent items of hardware that have compatible connectors enabling cross-connection. In other cases, an error trap will involve several factors that, in combination, can lead the operator to make a particular error—e.g., a difficult-to-reach non-captive fastener that must be tightened by a person wearing gloves who has no direct visual access to the fastener.

Because they apply to specific tasks, interfaces, and equipment, descriptions of error traps are likely to suggest possible solutions. Here are some examples of error traps:

- A warning in a procedure document appears after the procedural step to which it applies.
- Two components that are physically interchangeable but functionally different have similar labels or part numbers (e.g., NTS6132 and NTS1632).
- An input device provides no feedback to the operator that a command has been received, potentially leading to repetition of the command.
- A task requires the operator to perform an action opposite to habit, increasing the chance of a skill-based slip.

2.7 Develop and verify human error management strategy

Management strategies must be developed for human errors that could result in a catastrophic outcome. The aim of human error management is not necessarily to remove human error by assigning functions and tasks to machines (although in some cases, that may be appropriate). In many cases, it will be appropriate to take steps to protect the system from human error, while retaining the positive contribution of the human to system performance.

Human error management strategies are typically prioritized in the following order:

1. Prevent the error.
2. Reduce the likelihood of the error, and provide the capability to detect and correct or recover from it.
3. Limit the negative effect of the error.

Error management strategies may involve administrative or engineered countermeasures. Administrative countermeasures to error are “non-hardware” features of a system that rely on human behavior and compliance to prevent, detect, correct, and contain the effects of unwanted behavior. They typically take the form of procedures, paperwork, work practices, training, and warning signs.

Engineered countermeasures to error are built into the system. They include physical features such as covers, interlocks, and tethers, as well as software features such as “undo” buttons and validation checks to capture data entry errors.

When designing error management strategies, the following issues should be considered:

- Defense-in-depth. In some situations, it will be appropriate to have layers of defenses against a catastrophic error.
- Diversity of defenses. Adding diversity within the layer of defenses will generally provide more protection than simply repeating an existing defense (e.g., in some circumstances, an independent inspection plus a functional check may be more effective than two inspections or two functional checks).
- Matching countermeasures to errors. Ensuring that countermeasures are appropriate for the type of error. Different types of cognitive error (e.g., memory lapses vs. mistakes of controlled processing) require different interventions.
- Delayed vs. immediate consequences of error. If there is no delay between error and consequence, some interventions, such as secondary checks or inspections, may not be feasible. Some errors with delayed consequences will be immediately apparent and outwardly noticeable, whereas others will be latent (i.e., difficult to detect).
- Administrative vs. engineered countermeasures. Administrative defenses against error, such as procedures and warnings, typically rely on operator compliance and may not provide the same level of protection as engineered defenses, such as physical lockouts.

Proposed error management strategies should be verified to ensure they are effective in an operational context. The specific methods used for verification depend on the type of error management strategy. Verification methods include reviews by SMEs (including workers), comparison to requirements and human factors engineering guidance, and performance testing.

3. DOCUMENTING THE HEA

The HEA report should be seen as a living document that is updated regularly and referred to throughout system development. During the early stages of development, the HEA report may cover potential errors at a relatively coarse level. However, as the design and development phase proceeds, it should be possible to identify potential errors with more granularity, and the HEA report should reflect this.

The HEA team may choose to divide the report into two sections, as follows.

The first section of the HEA report may provide an overview of the activities outlined in the HSI plan, how they were used to identify potential human error, and the system improvements that resulted from these activities. In many cases, the system design team will have already identified and addressed the most obvious human errors. This section will typically describe the HSI activities that occurred during system development, including the application of human factors standards, crew workload evaluations, human-in-the-loop usability evaluations, and hazard assessments. This section may refer to other activities, such as safety analyses, and may also contain:

- A review of relevant information from other analyses that were made available to the HEA team.
- A description of how the planned HSI and analysis activities enabled identification of potential catastrophic errors.
- A list of system improvements made to address human error.
- A description of the evaluation activities performed to verify that the error mitigation strategies were successful.

The second section should describe the HEA approach taken to identify potentially catastrophic errors not captured by the activities outlined in the HSI plan, and the system improvements that occurred as a result of the HEA. System improvements may include changes to the design of hardware, procedures, or training. This section may contain:

- The screening approach used to identify areas for analysis.
- The method used to identify human tasks.
- The methods used to analyze errors.
- A description of catastrophic errors identified during the HEA.

- System improvements made as a result of the HEA.

4. CONCLUSIONS

There is no one way to conduct an HEA, and the team responsible must use judgment to identify the approach best suited to the system being examined. HEA requires imagination and foresight to consider not only the human interactions that are expected to occur with systems, but also foreseeable but unplanned interactions that may ocur.

This paper has described HEA as a series of sequential steps. However, in practice, the HEA process may not be entirely linear. Later steps in the process may bring to light information that requires earlier steps to be revisited. For example, when considering potential errors, it may become apparent that a task step has been overlooked in earlier task analyses.

HEA is not performed in isolation, but draws on other analyses, including hazard analysis and probabilistic risk assessment. A thorough HEA will identify previously unidentified areas of concern that will need to be included in these other analyses.

The HEA team should be aware that interventions intended to manage the risk of human error can sometimes present hazards in themselves. Modifications for preventing or mitigating error should be re-evaluated to ensure that issues have been addressed and that no new error vulnerabilities have been introduced.

Of course, there is no guarantee that HEA will uncover and control all the significant errors that could threaten a system. Nevertheless, in the absence of a HEA, systems are more likely to be vulnerable to hazards resulting from uncontrolled human errors.

5. REFERENCES

1. Aerospace Accident Report NTSB/AAR-15/02. National Transportation Safety Board.

2. NPR 8705.2C, Human-Rating Requirements for Space Systems. National Aeronautics and Space Administration.

3. Null, C., Hobbs, A., O'Hara, J., and Dischinger, C. (2019). Guidance for Human Error Analysis (HEA) NASA Engineering Safety Center Position Paper NESC-NPP-18-01368.

4. Leveson, N, and Thomas, J. (2018). STPA Handbook. Available at: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

5. Leary, W. (2004). Shuttle Flew for Decades With Potentially Fatal Flaw. *New York Times,* March 23, p 20.

6. Oberg, J. (2004). Space station leak caused by crew. NBC News. Available at https://www.nbcnews.com/id/wbna3969567

7. Kirwan, B., and Ainsworth, L.K. (1992). A guide to task analysis. London: Taylor and Francis.

8. Seamster, T.L., and Redding, R.E. (2017). Applied cognitive task analysis in aviation. London: Routledge.

9. Reason, J. (2004). Beyond the organizational accident: the need for "error wisdom" on the frontline. BMJ Quality & Safety, 13 (suppl 2), ii28-ii33.

10. Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method (CREAM). New York: Elsevier.

11. Reason, J. (1990). Human Error. Cambridge, UK: Cambridge University Press.

12. Null, C. (2018). Human Error Taxonomies. In Kanki, B.; Clervoy, J.; and Sandal, G. (Eds). Space Safety and Human Performance (pp. 36-52). Oxford: Butterworth Heinemann.

13. Shiffrin, R. M., & Schneider, W. (1977). Controlled and automatic human information processing: II. Perceptual learning, automatic attending, and a general theory. Psychological Review, 84, 127–190.